CLAIMS

1. An information recording medium recording contents encrypted using a content encryption key, and a content decryption key used for decrypting the encrypted contents and encrypted by an encryption key for decryption key, wherein

the encryption key for decryption key is different for each of the regions preset for at least controlling the permission and inhibition of playback of the contents,

the content encryption key and the content decryption key are established corresponding to each of the regions where the content playback is permitted, or corresponding to the combination of the regions where content playback is permitted.

2. An information recording medium according to claim 1, wherein the content decryption key is encrypted by the one or more encryption keys for decryption key provided corresponding to the playback device with which the content playback is permitted.

3. An information recording medium according to claim 1, wherein header information indicating the kind of the encryption key for decryption key is further recorded therein.

4. An information recording medium according to claim 1, wherein the content encryption key and the content decryption key belong to an region where content playback is permitted, and are established corresponding to a combination of playback devices with which the content playback is permitted.

5. An information recording medium according to claim 1, wherein, when the content playback in a predetermined playback device is newly revoked, the content encryption key and the content decryption key are renewed to a new key respectively.

6. An information recording medium according to claim 1, wherein the encryption keys for decryption key are managed by a key management system using one or more tree structures provided independently for the each region.

7. An information recording medium according to claim 6, wherein the encryption keys for decryption key are managed by a key management system employing one or more tree structures for each of the regions in the state in which one encryption key specified for region independently provided to each of the regions is a root and encryption keys specified for playback device provided to each of the playback devices are the leaves.

8. An information recording medium according to claim 6, wherein each of the tree structures employs an n-divided tree ($n \geq 2$).

9. An information recording medium according to claim 6, wherein the encryption keys for decryption key are managed by a key management system employing an n-divided tree ($n \geq 2$) in the state in which one encryption key specified for region independently provided to each of the regions is a root and encryption keys specified for playback device, provided to each of the playback devices are the leaves.

10. An information recording device, comprising:

a content encryption key inputting section for establishing and inputting a content encryption key corresponding to each of the regions where playback of the contents is permitted, or corresponding to combination of the regions where content playback is permitted;

a content decryption key inputting section for establishing and inputting a content decryption key utilized for decrypting the contents encrypted by the content encryption key;

an encryption key for decryption key selecting section for selecting an encryption key for decryption key corresponding to the region where playback of the contents is permitted;

a content encryption section for encrypting the contents utilizing the content encryption key;

a content decryption key encrypting section for encrypting the content decryption key using the encryption key for decryption key, and

a recording section for recording at least the encrypted contents and the encrypted content decryption key to an information recording medium.

11. An information playback device for playing information including contents encrypted utilizing a content encryption key, and a content decryption key used for decrypting the encrypted contents and encrypted by an encryption key for decryption key, comprising:

a decryption key storing section storing a decryption key for decryption key for decrypting the content decryption key encrypted by the encryption key for decryption key;

a content decryption key decrypting section for decrypting the content decryption key by using the decryption key for decryption key;

a content decrypting section for decrypting the contents by utilizing the content decryption key, and

a playback section for playing the decrypted contents, wherein

the decryption keys for decryption key is different for each of the regions preset for at least controlling the permission and inhibition of the content playback,

the content encryption key and the content decryption key are established corresponding to each of the regions where content playback is permitted, or corresponding to the combination of the regions where content playback is permitted.

12. An information playback device according to claim 11, wherein the decryption key storing section stores therein plural kinds of decryption keys for decryption key including decryption keys specified for region established corresponding to regions where information playback devices belong to, and decryption keys specified for playback device allotted to each of the information playback devices.

13. An information playback device according to 12, wherein the plural kinds of decryption keys for decryption key are allotted and stored to each of the playback devices with the management of a key

management system employing one or more tree structures independently provided for each of the regions.

14. An information playback device according to 13, wherein the decryption key for decryption key are managed by a key management system employing one or more tree structures for each of the regions in a state that a decryption key specified for region independently provided to each of the regions is the root and the decryption keys specified for playback device provided to each of the playback devices are leaves.

15. An information delivery device comprising:

a delivery section for delivering contents encrypted utilizing a content encryption key, and content decryption key used for decrypting the encrypted contents and encrypted by an encryption key for decryption key.

16. An information recording method, comprising the steps of:

obtaining selection information of the regions where playback of the contents is permitted;

establishing a content encryption key and a content decryption key corresponding to the selected regions or the combination thereof,

obtaining an encryption key for decryption key preset in accordance with the selected region,

encrypting the contents utilizing the content encryption key,

encrypting the content decryption key using the encryption key for decryption key, and

recording the encrypted contents and the encrypted content decryption key to an information recording medium.

17. An information recording method according to claim 16, further comprising a step of

establishing the encryption key for decryption key with a combination having the number smallest in a group of the encryption keys for decryption key, in which the encryption keys for decryption key owned by playback devices being permitted to play in a selected region is included, and

the encryption key for decryption key owned by playback device being prohibited from playing is not included.

18. An information playback method for playing information including contents encrypted utilizing a content encryption key, and a content decryption key used for decrypting the encrypted contents and encrypted by an encryption key for decryption, wherein

the decryption key for decryption key is different for each of the regions preset at least for controlling the permission and inhibition of the content playback,

the content encryption key and the content decryption key are established corresponding to the each of the regions where content playback is permitted or, in accordance with the combination of regions where content playback is permitted,

the method comprising the steps of:

checking whether or not an information playback device has a decryption key for decryption key corresponding to the encryption key for decryption key encrypting the content decryption key,

decrypting the content decryption key using the decryption key for decryption key when the information playback device has the corresponding decryption key for decryption key,

decrypting the contents utilizing the decrypted content decryption key, and

playing the decrypted contents.

19. An information recording program, wherein the program causes a computer to execute the information recording method set forth in claim 16.

20. An information playback program, wherein the program causes a computer to execute the information playback method set forth in claim 18.

21. A recording medium recording an information recording program, wherein the information recording program set forth in claim 19 is recorded so as to be read out by a computer.

22. A recording medium recording an information playback program, wherein the information playback program set forth in claim 20 is recorded so as to be read out by a computer.